Information & Communication Technology (ICT) - KEEPING SAFE ONLINE

Policy Number	0019	Completed by	Imogen Morgan Clare	Last Reviewed date	13/02/2026
Version Number	0001	Signed off by	Adrian Stenner	Next Review date	13/02/2027

POLICY STATEMENT OF INTENT

This policy outlines the procedures we have in place within Skylark to ensure that our students and staff are able to keep themselves safe online.

INTRODUCTION

New technologies have become integral to the lives of children and adults in today's society, both within the educational and enrichment provisions of Skylark and in their outside lives.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps instructors and pupils/students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and adults should have an entitlement to safe internet access.

SCOPE AND AIMS

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely, is addressed as part of the wider duty of care to which all who work at Skylark are bound.

POLICY

Appropriate use of these exciting and innovative tools in the educational and residential provisions, has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put children and adults at risk within and outside the provision.
Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to / loss of / sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing / distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication / contact with others, including strangers;
- Cyber-bullying;
- Access to unsuitable video / internet games;

- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person;
- Potential for radicalisation through inappropriate content or contact

As with all risks, it is impossible to eliminate them completely. It is therefore essential, through good education, to build pupils'/students' resilience to the risks to which they may be exposed, so that they have the confidence and skills, to face and deal with these risks.

Skylark will provide the necessary safeguards, to help ensure that it has done everything that could reasonably be expected of it, to manage and reduce these risks.

This Online Safety Policy, explains how it intends to manage risk, while also addressing wider educational issues, in order to help young people to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

PROCEDURE

Pupils/Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety, is therefore an essential part of

Skylark's online safety provision. Children and young people, need the help and support of their provision to recognise and avoid online safety risks and build their resilience.

Online Safety education will be provided in the following ways:

- Key online safety messages should be reinforced as part of a planned programme of tutorials and activities;

- Pupils/students should be taught in relevant sessions to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information;

- Pupils/students should be helped to understand the need for the student and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside their educational and care provision;

- Pupils/students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;

- Pupils/students should be taught the dangers that can exist through the use of inappropriate websites, and the potential of on-line grooming for exploitation or radicalisation purposes;

- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Staff - education & training

- This Online Safety Policy and its updates will be presented to and discussed at relevant team meetings
- Skylark Will be responsible for ensuring that any network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented;
- Regular reviews and audits of the safety and security of Trust ICT systems;
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- Personal data may not be sent over the internet or taken away from a Trust site unless safely encrypted or otherwise secured.

SAFEGUARDING YOURSELF AS AN EMPLOYEE OR VOLUNTEER OF SKYLARK

Guidance on the personal use of social networking sites for adults involved in services for children, young people and vulnerable adults.

Due to the increasing personal use of social networking sites, staff and volunteers within the workforce should be aware of the impact of their personal use upon their professional position.

In practice, anything posted on the internet will be there forever and is no longer in your control. Remember when something is on the internet even if you remove it, it may have already been “snapshotted” by a “web crawler” and so will always be there.

Current and future employers and service users may see this. Keep all professional work completely separate from your private life.

The following guidance, in addition to the above, will safeguard adults from allegations and protect an individual’s privacy, as well as safeguard vulnerable groups.

Skylark expects all staff to comply with the following (the failure of which, may result in Skylark taking disciplinary action):

- Social networking sites such as Facebook have a range of privacy settings which are often set up to ‘expose’ your details to anyone. When ‘open’ anyone can find you from a search of the social networking site or even from a Google search. Therefore, it is important to change your setting to ‘just friends’ so that your details, comments, and photographs can only be seen by your invited friends.

- Have a neutral picture of yourself as your profile image.

- Do not post embarrassing material or comments that may call into question your employment status, this includes anything that is confidential or sensitive, including information about pupils/students or ex-pupils/ex-students, any information that is intended for internal use only (including matters concerning provision services, organisational change or related proposals).

- You should always show respect to others when using social media. You must never criticise Skylark, its pupils/students and staff, or anyone else you come into contact with professionally.

- Do not use personal social media to raise or discuss a complaint or grievance about Skylark, your manager, colleagues etc. There are formal grievance procedures for progressing these within the Trust.

- Do not accept friendship requests unless you know the person or want to accept them.

- Choose your social networking friends carefully and ask about their privacy controls.

- Be prepared for being bombarded with friendship requests from people you do not know.

- Do not accept friendship requests on social networking or messaging sites from pupils/students or ex-pupils/ex-students (or their parents/carers) that you work with.

- For those working with young people, remember that ex-pupils/ex-students may still have friends that you may have contact with through your work.

- Exercise caution. For example, if you write on a friends ‘wall’ on Facebook, all of their own friends can see your comment even if they are not your friend.

- There is a separate privacy setting for Facebook groups and other similar networks.

- You may have your own profile set to private, however, when joining a group or a network please be aware that everyone in that group or network is able to see your profile.

- If you have younger friends or family members on your social networking groups who are friends with pupils/students (or their parents/carers) that you work with, be aware that posts you write will be visible to them.

- Do not use your personal or professional details (email or telephone) as part of your profile.

- If you or a friend are tagged in an online photo album (Facebook, flickr etc.) the whole photo album may be visible to their friends, your friends and anyone else tagged in the photo album.

- You do not have to be friends with anyone to be tagged in their photo album, if you are tagged in a photo you can remove the tag but not the photo.

- You should be aware of the privacy settings on photo sharing websites.

- Your friends may take and post photos that you may not be happy about. You need to speak to them first to request that it is removed rather than contacting the web provider. If you are over the age of 18, the website will only look into issues that contravene their terms and conditions.

- Do not use your personal profile in any way for official business. If you are going to be a friend of Skylark's official social networking group, ensure you have a separate professional profile.

- If you have concerns related to radicalisation or on-line grooming, then please contact the local safeguarding lead.

- If you have difficulty in implementing any of this guidance, contact the local safeguarding lead.